Introduction à la cryptographie

AbdelAli SAIDI

Grande École Marocaine de l'Informatique et des Télécoms

2012/2013

abdelali.saidi@gmail.com

Plan

Plan

Terminologie

La cryptologie

Qu'est ce que la cryptologie?

Composantes

Terminologie

La cryptologie

Qu'est ce que la cryptologie?

La cryptologie est *l'art du secret*. Elle consiste à dissimuler l'information même si elle est accessible.

Composantes

Terminologie
La cryptologie

Qu'est ce que la cryptologie?

La cryptologie est *l'art du secret*. Elle consiste à dissimuler l'information même si elle est accessible.

Composantes

La cryptologie se compose de deux disciplines complémentaires:

Terminologie
La cryptologie

Qu'est ce que la cryptologie?

La cryptologie est *l'art du secret*. Elle consiste à dissimuler l'information même si elle est accessible.

Composantes

La cryptologie se compose de deux disciplines complémentaires:

- La cryptographie

Terminologie
La cryptologie

Qu'est ce que la cryptologie?

La cryptologie est *l'art du secret*. Elle consiste à dissimuler l'information même si elle est accessible.

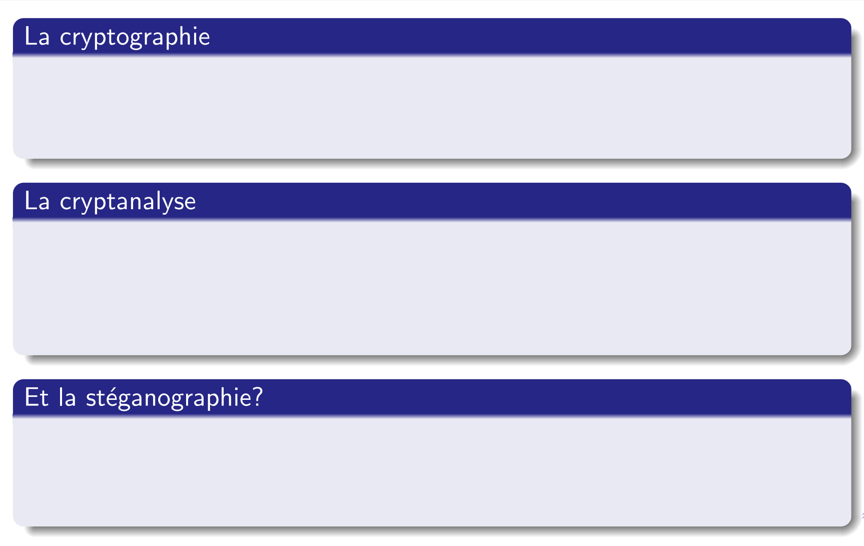
Composantes

La cryptologie se compose de deux disciplines complémentaires:

- La cryptographie
- La cryptanalyse

Terminologie

La cryptographie et la cryptanalyse



Terminologie

La cryptographie et la cryptanalyse

La cryptographie

La cryptographie est l'étude et la pratique de techniques qui permettent de sécuriser une information même en présence d'une personne non autorisée.

La cryptanalyse

Et la stéganographie?

Terminologie

La cryptographie et la cryptanalyse

La cryptographie

La cryptographie est l'étude et la pratique de techniques qui permettent de sécuriser une information même en présence d'une personne non autorisée.

La cryptanalyse

La cryptanalyse est l'ensemble des techniques qui permettent de tester la force de la cryptographie. En d'autres mots, l'objectif de la cryptanalyse est de déterminer, de façon illégitime, le contenu d'une information chiffrée.

Et la stéganographie?

Terminologie

La cryptographie et la cryptanalyse

La cryptographie

La cryptographie est l'étude et la pratique de techniques qui permettent de sécuriser une information même en présence d'une personne non autorisée.

La cryptanalyse

La cryptanalyse est l'ensemble des techniques qui permettent de tester la force de la cryptographie. En d'autres mots, l'objectif de la cryptanalyse est de déterminer, de façon illégitime, le contenu d'une information chiffrée.

Et la stéganographie?

La stéganographie est aussi un *art du secret*. À l'encontre de la cryptographie, elle consiste seulement à faire passer une information secrète dans une autre comme leurre.

Terminologie

- *Texte en clair*:
- *Texte chiffré*:
- *Chiffrement*:
- *Déchiffrement*:
- *Clé*:

Terminologie

- *Texte en clair*: On désigne par *texte en clair* l'information secrète
- *Texte chiffré*:
- *Chiffrement*:
- *Déchiffrement*:
- *Clé*:

Terminologie

- *Texte en clair*: On désigne par *texte en clair* l'information secrète
- *Texte chiffré*: Est l'image non compréhensible du *texte en clair*
- *Chiffrement*:
- *Déchiffrement*:
- *Clé*:

Terminologie

- *Texte en clair*: On désigne par *texte en clair* l'information secrète
- *Texte chiffré*: Est l'image non compréhensible du *texte en clair*
- *Chiffrement*: Est la transformation du *texte en clair* en un *texte chiffré*
- *Déchiffrement*:
- *Clé*:

Terminologie

- *Texte en clair*: On désigne par *texte en clair* l'information secrète
- *Texte chiffré*: Est l'image non compréhensible du *texte en clair*
- *Chiffrement*: Est la transformation du *texte en clair* en un *texte chiffré*
- *Déchiffrement*: L'opération inverse du *chiffrement*
- *Clé*:

Terminologie

- *Texte en clair*: On désigne par *texte en clair* l'information secrète
- *Texte chiffré*: Est l'image non compréhensible du *texte en clair*
- *Chiffrement*: Est la transformation du *texte en clair* en un *texte chiffré*
- *Déchiffrement*: L'opération inverse du *chiffrement*
- *Clé*: L'outil du *chiffrement* et/ou du *déchiffrement*

Historique

Spartan scytale (150 B.C.)



Spartan scytale (150 B.C.)

Historique

Spartan scytale (150 B.C.)



Spartan scytale (150 B.C.)

- Utilisation d'une lanière avec un bâton(scytale) de diamètre fixe

Historique
Spartan scytale (150 B.C.)



Spartan scytale (150 B.C.)

- Utilisation d'une lanière avec un bâton(scytale) de diamètre fixe
- Pour cela, l'expéditeur:

Historique

Spartan scytale (150 B.C.)



Spartan scytale (150 B.C.)

- Utilisation d'une lanière avec un bâton(scytale) de diamètre fixe
- Pour cela, l'expéditeur:
  - partage le diamètre du bâton avec le destinataire seul

Historique

Spartan scytale (150 B.C.)



Spartan scytale (150 B.C.)

- Utilisation d'une lanière avec un bâton(scytale) de diamètre fixe
- Pour cela, l'expéditeur:
  - partage le diamètre du bâton avec le destinataire seul
  - roule la lanière sur le bâton

Historique

Spartan scytale (150 B.C.)



Spartan scytale (150 B.C.)

- Utilisation d'une lanière avec un bâton(scytale) de diamètre fixe
- Pour cela, l'expéditeur:
    - partage le diamètre du bâton avec le destinataire seul
    - roule la lanière sur le bâton
    - écrit le texte en clair sur la lanière

Historique

Spartan scytale (150 B.C.)



Spartan scytale (150 B.C.)

- Utilisation d'une lanière avec un bâton(scytale) de diamètre fixe
- Pour cela, l'expéditeur:
  - partage le diamètre du bâton avec le destinataire seul
  - roule la lanière sur le bâton
  - écrit le texte en clair sur la lanière
  - déroule la lanière et l'envoie au destinataire

Historique

Spartan scytale (150 B.C.)



Spartan scytale (150 B.C.)

- Utilisation d'une lanière avec un bâton(scytale) de diamètre fixe
- Pour cela, l'expéditeur:
  - partage le diamètre du bâton avec le destinataire seul
  - roule la lanière sur le bâton
  - écrit le texte en clair sur la lanière
  - déroule la lanière et l'envoie au destinataire
- Le destinataire doit utiliser un bâton du même diamètre pour le déchiffrement

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

Exemple

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*

Exemple

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*
- Elle consiste à décaler les lettres du *texte en clair* de trois positions

Exemple

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*
- Elle consiste à décaler les lettres du *texte en clair* de trois positions
- Pour cela, l'expéditeur:

Exemple

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*
- Elle consiste à décaler les lettres du *texte en clair* de trois positions
- Pour cela, l'expéditeur:
  - partage le nombre de décalage avec le destinataire seul

Exemple

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*
- Elle consiste à décaler les lettres du *texte en clair* de trois positions
- Pour cela, l'expéditeur:
  - partage le nombre de décalage avec le destinataire seul
  - procède au décalage

Exemple

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*
- Elle consiste à décaler les lettres du *texte en clair* de trois positions
- Pour cela, l'expéditeur:
  - partage le nombre de décalage avec le destinataire seul
  - procède au décalage
  - envoie le résultat au destinataire

Exemple

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*
- Elle consiste à décaler les lettres du *texte en clair* de trois positions
- Pour cela, l'expéditeur:
  - partage le nombre de décalage avec le destinataire seul
  - procède au décalage
  - envoie le résultat au destinataire
- Le destinataire procède à une substitution inverse

Exemple

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*
- Elle consiste à décaler les lettres du *texte en clair* de trois positions
- Pour cela, l'expéditeur:
  - partage le nombre de décalage avec le destinataire seul
  - procède au décalage
  - envoie le résultat au destinataire
- Le destinataire procède à une substitution inverse

Exemple

Texte en clair: rendons a cesar ce qui est a cesar
Texte chiffré:

Historique

Caesar's cipher (100 B.C.)

Caesar's cipher (100 B.C.)

- C'est une méthode de chiffrement par *substitution mono-alphabétique*
- Elle consiste à décaler les lettres du *texte en clair* de trois positions
- Pour cela, l'expéditeur:
  - partage le nombre de décalage avec le destinataire seul
  - procède au décalage
  - envoie le résultat au destinataire
- Le destinataire procède à une substitution inverse

Exemple

Texte en clair:	rendons a cesar ce qui est a cesar
Texte chiffré:	UHQGRQV D FGVDU FH TYM GVW D FGVDU

Historique

La machine Enigma



- Cette machine a été utilisé par les Nazis durant la deuxième guerre mondiale
- Son algorithme a été cassé en 1932 par les alliés (les polonais et les anglais)

Historique

Principe de Kerckhoffs

Le principe

Conséquences

Historique
Principe de Kerckhoffs

Le principe

- L'algorithme doit être public et seules les clés sont secrètes.

Conséquences

Historique
Principe de Kerckhoffs

Le principe

- L'algorithme doit être public et seules les clés sont secrètes.

Conséquences

- La sécurité de l'information reposera alors seulement sur le secret de la clé utilisée

Historique

Principe de Kerckhoffs

Le principe

- L'algorithme doit être public et seules les clés sont secrètes.
- Le déchiffrement sans la clé ne doit être possible qu'après un moment raisonnable

Conséquences

- La sécurité de l'information reposera alors seulement sur le secret de la clé utilisée

Historique

Principe de Kerckhoffs

Le principe

- L'algorithme doit être public et seules les clés sont secrètes.
- Le déchiffrement sans la clé ne doit être possible qu'après un moment raisonnable

Conséquences

- La sécurité de l'information reposera alors seulement sur le secret de la clé utilisée
- Trouver la clé à partir des textes en clair et chiffré ne doit être possible qu'après un moment raisonnable

Plan

La substitution

La substitution mono-alphabétique

Définition

Formule générale

La substitution

La substitution mono-alphabétique

Définition

La substitution est le remplacement d'une lettre du texte en clair par une autre lettre. Les lettres générées par ces remplacements forment le texte chiffré.

Formule générale

La substitution

La substitution mono-alphabétique

Définition

La substitution est le remplacement d'une lettre du texte en clair par une autre lettre. Les lettres générées par ces remplacements forment le texte chiffré.

Formule générale

Chaque lettre c du texte chiffré correspond à une lettre a du texte en clair selon la formule suivante.

$$c_i = a_i + k[n]$$

La substitution

La substitution mono-alphabétique

Définition

La substitution est le remplacement d'une lettre du texte en clair par une autre lettre. Les lettres générées par ces remplacements forment le texte chiffré.

Formule générale

Chaque lettre c du texte chiffré correspond à une lettre a du texte en clair selon la formule suivante.

$$c_i = a_i + k[n]$$

- k: le nombre de décalage
- n: la dimension de l'ensemble auquel appartient les lettres

La substitution

La substitution mono-alphabétique

Exemple (Caesar's cipher)

La substitution

La substitution mono-alphabétique

Exemple (Caesar's cipher)

Texte en clair	rendons a cesar ce qui est a cesar
Texte chiffré	UHQGRQV D FGVDU FH TYM GVW D FGVDU

La substitution
La substitution mono-alphabétique

Exemple (Caesar's cipher)

Texte en clair	rendons a cesar ce qui est a cesar
Texte chiffré	UHQGRQV D FGVDU FH TYM GVW D FGVDU

Avec k=3 et n=26

La substitution

La substitution poly-alphabétique

Définition

Formule générale

Exemple

La substitution

La substitution poly-alphabétique

Définition

C'est une amélioration de la méthode précédente. Ici, le “k” est variable.

Formule générale

Exemple

La substitution

La substitution poly-alphabétique

Définition

C'est une amélioration de la méthode précédente. Ici, le "k" est variable.

Formule générale

$$c_i = a_i + k_i[n]$$

Exemple

La substitution

La substitution poly-alphabétique

Définition

C'est une amélioration de la méthode précédente. Ici, le “k” est variable.

Formule générale

$$c_i = a_i + k_i[n]$$

Exemple

Table de vigenère

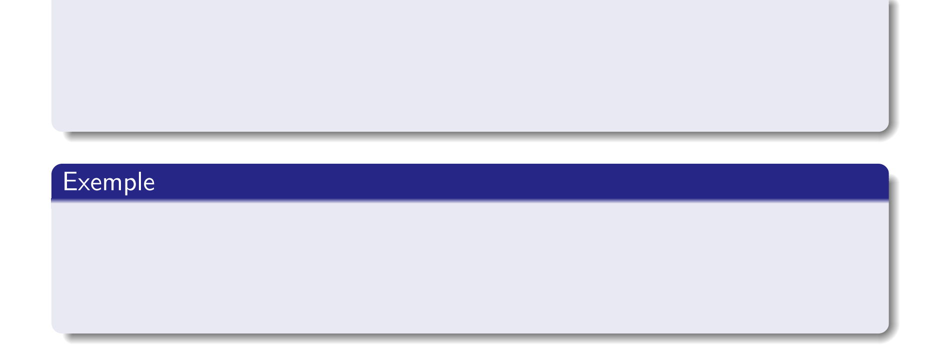
La substitution

La substitution poly-alphabétique

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure: Table de vigenère

La substitution
La substitution poly-alphabétique



La substitution

La substitution poly-alphabétique

- L'expéditeur et le destinataire doivent se mettre d'accord sur un mot clé qui représentera l'ensemble de k

Exemple

La substitution

La substitution poly-alphabétique

- L'expéditeur et le destinataire doivent se mettre d'accord sur un mot clé qui représentera l'ensemble de k
- Ce mot clé est répété autant de fois selon la longueur du texte en clair

Exemple

La substitution

La substitution poly-alphabétique

- L'expéditeur et le destinataire doivent se mettre d'accord sur un mot clé qui représentera l'ensemble de k
- Ce mot clé est répété autant de fois selon la longueur du texte en clair

Exemple

Texte en clair	rendons a cesar ce qui est a cesar
Texte chiffré	

Sachant que : $k_i \in VINCI$

La substitution

La substitution poly-alphabétique

- L'expéditeur et le destinataire doivent se mettre d'accord sur un mot clé qui représentera l'ensemble de k
- Ce mot clé est répété autant de fois selon la longueur du texte en clair

Exemple

Texte en clair	rendons a cesar ce qui est a cesar
Texte chiffré	MMAFWIA N EMNIE EM LCV GAO I PGAVZ

Sachant que : $k_i \in VINCI$

La substitution

La substitution par polygrammes

La substitution par polygrammes

Exemple: Chiffre de Playfair (bigramme)

La substitution

La substitution par polygrammes

La substitution par polygrammes

La substitution procède par bloc de caractères.

Exemple: Chiffre de Playfair (bigramme)

La substitution

La substitution par polygrammes

La substitution par polygrammes

La substitution procède par bloc de caractères.

Exemple: Chiffre de Playfair (bigramme)

- Utilisation d'une matrice de lettres (5x5) combiné avec un mot clé

La substitution

La substitution par polygrammes

La substitution par polygrammes

La substitution procède par bloc de caractères.

Exemple: Chiffre de Playfair (bigramme)

- Utilisation d'une matrice de lettres (5x5) combiné avec un mot clé
- Cette combinaison fera l'objet de la clé de chiffrement et de déchiffrement

La substitution

La substitution par polygrammes

La substitution par polygrammes

La substitution procède par bloc de caractères.

Exemple: Chiffre de Playfair (bigramme)

- Utilisation d'une matrice de lettres (5x5) combiné avec un mot clé
- Cette combinaison fera l'objet de la clé de chiffrement et de déchiffrement
- Construction de la matrice:

La substitution

La substitution par polygrammes

La substitution par polygrammes

La substitution procède par bloc de caractères.

Exemple: Chiffre de Playfair (bigramme)

- Utilisation d'une matrice de lettres (5x5) combiné avec un mot clé
- Cette combinaison fera l'objet de la clé de chiffrement et de déchiffrement
- Construction de la matrice:
  - Inscrire horizontalement le mot clé dans la matrice en ignorant les doublons

La substitution

La substitution par polygrammes

La substitution par polygrammes

La substitution procède par bloc de caractères.

Exemple: Chiffre de Playfair (bigramme)

- Utilisation d'une matrice de lettres (5x5) combiné avec un mot clé
- Cette combinaison fera l'objet de la clé de chiffrement et de déchiffrement
- Construction de la matrice:
  - Inscrire horizontalement le mot clé dans la matrice en ignorant les doublons
  - Remplissage du reste des cases de la matrice avec le reste des alphabets (en respectant leur ordre)

La substitution

La substitution par polygrammes

La substitution par polygrammes

La substitution procède par bloc de caractères.

Exemple: Chiffre de Playfair (bigramme)

- Utilisation d'une matrice de lettres (5x5) combiné avec un mot clé
- Cette combinaison fera l'objet de la clé de chiffrement et de déchiffrement
- Construction de la matrice:
  - Inscrire horizontalement le mot clé dans la matrice en ignorant les doublons
  - Remplissage du reste des cases de la matrice avec le reste des alphabets (en respectant leur ordre)
  - Traiter I comme J

La substitution

Chiffre de Playfair (bigramme)

Chiffre de Playfair (bigramme)

Exemple

La substitution
Chiffre de Playfair (bigramme)

Chiffre de Playfair (bigramme)

- Règles du chiffrement:

Exemple

La substitution

Chiffre de Playfair (bigramme)

Chiffre de Playfair (bigramme)

- Règles du chiffrement:
  - On prend le message chiffré par blocs de deux lettres

Exemple

La substitution
Chiffre de Playfair (bigramme)

Chiffre de Playfair (bigramme)

- Règles du chiffrement:
  - On prend le message chiffré par blocs de deux lettres
  - Si les deux lettres occupent la même ligne, on les remplace par ceux qui se trouvent immédiatement à leur droite

Exemple

La substitution

Chiffre de Playfair (bigramme)

Chiffre de Playfair (bigramme)

- Règles du chiffrement:
  - On prend le message chiffré par blocs de deux lettres
  - Si les deux lettres occupent la même ligne, on les remplace par ceux qui se trouvent immédiatement à leur droite
  - Si les deux lettres occupent la même colonne, on les remplace par ceux qui sont juste à leur bas

Exemple

La substitution

Chiffre de Playfair (bigramme)

Chiffre de Playfair (bigramme)

- Règles du chiffrement:
  - On prend le message chiffré par blocs de deux lettres
  - Si les deux lettres occupent la même ligne, on les remplace par ceux qui se trouvent immédiatement à leur droite
  - Si les deux lettres occupent la même colonne, on les remplace par ceux qui sont juste à leur bas
  - Sinon, on prend les lettres qui se trouvent à l'intersection des lignes et colonnes des deux premières lettres

Exemple

La substitution

Chiffre de Playfair (bigramme)

Chiffre de Playfair (bigramme)

- Règles du chiffrement:
  - On prend le message chiffré par blocs de deux lettres
  - Si les deux lettres occupent la même ligne, on les remplace par ceux qui se trouvent immédiatement à leur droite
  - Si les deux lettres occupent la même colonne, on les remplace par ceux qui sont juste à leur bas
  - Sinon, on prend les lettres qui se trouvent à l'intersection des lignes et colonnes des deux premières lettres
  - Si les deux lettres sont identiques ou bien il n'en reste qu'une, on met un "x" après la première lettre

Exemple

La substitution

Chiffre de Playfair (bigramme)

Chiffre de Playfair (bigramme)

- Règles du chiffrement:
  - On prend le message chiffré par blocs de deux lettres
  - Si les deux lettres occupent la même ligne, on les remplace par ceux qui se trouvent immédiatement à leur droite
  - Si les deux lettres occupent la même colonne, on les remplace par ceux qui sont juste à leur bas
  - Sinon, on prend les lettres qui se trouvent à l'intersection des lignes et colonnes des deux premières lettres
  - Si les deux lettres sont identiques ou bien il n'en reste qu'une, on met un "x" après la première lettre

Exemple

Trouvez le texte en clair du texte chiffré "UI OI NP HU OI BG PN" sachant que k=SECURITY

La substitution

Masque jetable

Masque jetable

La substitution
Masque jetable

Masque jetable

Cette utilisation des clés renforce la sécurité des communications contre les attaques statistiques

La substitution

Masque jetable

Masque jetable

Cette utilisation des clés renforce la sécurité des communications contre les attaques statistiques

- Utilisation d'une seule clé par message

La substitution
Masque jetable

Masque jetable

Cette utilisation des clés renforce la sécurité des communications contre les attaques statistiques

- Utilisation d'une seule clé par message
- La clé est généré d'une manière aléatoire

La substitution

Masque jetable

Masque jetable

Cette utilisation des clés renforce la sécurité des communications contre les attaques statistiques

- Utilisation d'une seule clé par message
- La clé est généré d'une manière aléatoire
- La taille de la clé doit correspondre à la taille du message

La transposition

La transposition

La transposition

La transposition

- Le chiffrement par transposition est basé sur des permutations de caractères

La transposition

La transposition

- Le chiffrement par transposition est basé sur des permutations de caractères
- Les caractères du texte en clair constituent les caractères du texte chiffré

La transposition

La transposition

- Le chiffrement par transposition est basé sur des permutations de caractères
- Les caractères du texte en clair constituent les caractères du texte chiffré
- On commence par remplir une matrice par le texte en clair et on chiffre en utilisant:

La transposition

La transposition

- Le chiffrement par transposition est basé sur des permutations de caractères
- Les caractères du texte en clair constituent les caractères du texte chiffré
- On commence par remplir une matrice par le texte en clair et on chiffre en utilisant:
  - Transposition simple

La transposition

La transposition

- Le chiffrement par transposition est basé sur des permutations de caractères
- Les caractères du texte en clair constituent les caractères du texte chiffré
- On commence par remplir une matrice par le texte en clair et on chiffre en utilisant:
  - Transposition simple
  - Transposition complexe

La transposition

Transposition simple

Transposition simple

Exemple



La transposition
Transposition simple

Transposition simple

- L'ordre de la matrice constitue la clé

Exemple

La transposition

Transposition simple

Transposition simple

- L'ordre de la matrice constitue la clé
- Le message est écrit sur la matrice horizontalement

Exemple

La transposition

Transposition simple

Transposition simple

- L'ordre de la matrice constitue la clé
- Le message est écrit sur la matrice horizontalement
- On complète la matrice par la lettre X

Exemple

La transposition

Transposition simple

Transposition simple

- L'ordre de la matrice constitue la clé
- Le message est écrit sur la matrice horizontalement
- On complète la matrice par la lettre X
- Le message chiffré est obtenu en lisant la matrice verticalement

Exemple

La transposition
Transposition simple

Transposition simple

- L'ordre de la matrice constitue la clé
- Le message est écrit sur la matrice horizontalement
- On complète la matrice par la lettre X
- Le message chiffré est obtenu en lisant la matrice verticalement

Exemple

k = 4x4, texte en clair = securite des si

La transposition

Transposition simple

Transposition simple

- L'ordre de la matrice constitue la clé
- Le message est écrit sur la matrice horizontalement
- On complète la matrice par la lettre X
- Le message chiffré est obtenu en lisant la matrice verticalement

Exemple

k = 4x4, texte en clair = securite des si

1	*2*	*3*	*4*	
s	e	c	u	
r	i	t	e	$\Longrightarrow$
d	e	s	s	
i	x	x	x	

La transposition

Transposition simple

Transposition simple

- L'ordre de la matrice constitue la clé
- Le message est écrit sur la matrice horizontalement
- On complète la matrice par la lettre X
- Le message chiffré est obtenu en lisant la matrice verticalement

Exemple

k = 4x4, texte en clair = securite des si

1	*2*	*3*	*4*
s	e	c	u
r	i	t	e
d	e	s	s
i	x	x	x

$\Longrightarrow$ texte chiffré = SRDI EIEX CTSX UESX

La transposition

Transposition complexe

Transposition complexe

Exemple

La transposition

Transposition complexe

Transposition complexe

- Ici, la clé de la transposition dépend d'un mot clé aussi

Exemple

La transposition

Transposition complexe

Transposition complexe

- Ici, la clé de la transposition dépend d'un mot clé aussi
- Ce mot clé fixe le nombre de colonnes de la matrice

Exemple

La transposition

Transposition complexe

Transposition complexe

- Ici, la clé de la transposition dépend d'un mot clé aussi
- Ce mot clé fixe le nombre de colonnes de la matrice
- Le nombre de lignes dépend de la taille du texte en clair

Exemple

La transposition

Transposition complexe

Transposition complexe

- Ici, la clé de la transposition dépend d'un mot clé aussi
- Ce mot clé fixe le nombre de colonnes de la matrice
- Le nombre de lignes dépend de la taille du texte en clair
- Le mot ne doit pas contenir des doublons

Exemple

La transposition
Transposition complexe

Transposition complexe

- Ici, la clé de la transposition dépend d'un mot clé aussi
- Ce mot clé fixe le nombre de colonnes de la matrice
- Le nombre de lignes dépend de la taille du texte en clair
- Le mot ne doit pas contenir des doublons
- Le texte chiffré est ordonné selon l'ordre des lettres du mot clé

Exemple

La transposition

Transposition complexe

Transposition complexe

- Ici, la clé de la transposition dépend d'un mot clé aussi
- Ce mot clé fixe le nombre de colonnes de la matrice
- Le nombre de lignes dépend de la taille du texte en clair
- Le mot ne doit pas contenir des doublons
- Le texte chiffré est ordonné selon l'ordre des lettres du mot clé

Exemple

k = INFO, texte en clair = securite des si

La transposition

Transposition complexe

Transposition complexe

- Ici, la clé de la transposition dépend d'un mot clé aussi
- Ce mot clé fixe le nombre de colonnes de la matrice
- Le nombre de lignes dépend de la taille du texte en clair
- Le mot ne doit pas contenir des doublons
- Le texte chiffré est ordonné selon l'ordre des lettres du mot clé

Exemple

k = INFO, texte en clair = securite des si

I	N	F	O	
s	e	c	u	
r	i	t	e	$\Longrightarrow$
d	e	s	s	
i	x	x	x	

La transposition

Transposition complexe

Transposition complexe

- Ici, la clé de la transposition dépend d'un mot clé aussi
- Ce mot clé fixe le nombre de colonnes de la matrice
- Le nombre de lignes dépend de la taille du texte en clair
- Le mot ne doit pas contenir des doublons
- Le texte chiffré est ordonné selon l'ordre des lettres du mot clé

Exemple

k = INFO, texte en clair = securite des si

I	N	F	O
s	e	c	u
r	i	t	e
d	e	s	s
i	x	x	x

$\Longrightarrow$ texte chiffré = CTSX SRDI EIEX UESX

Plan

La cryptographie moderne

La cryptographie moderne

- Elle repose uniquement sur les mathématiques

La cryptographie moderne

- Elle repose uniquement sur les mathématiques
- On chiffre des nombres binaires

La cryptographie moderne

- Elle repose uniquement sur les mathématiques
- On chiffre des nombres binaires
- Son algorithme de chiffrement doit être publié

La cryptographie moderne

- Elle repose uniquement sur les mathématiques
- On chiffre des nombres binaires
- Son algorithme de chiffrement doit être publié
- La confidentialité du message doit ne reposer que sur la clé

La cryptographie moderne

- Elle repose uniquement sur les mathématiques
- On chiffre des nombres binaires
- Son algorithme de chiffrement doit être publié
- La confidentialité du message doit ne reposer que sur la clé
- La communauté pourra alors tester sa robustesse afin de l'améliorer

Objectifs de la cryptographie

Principes de la sécurité

Modes de chiffrement

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*

Modes de chiffrement

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*

Modes de chiffrement

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*

Modes de chiffrement

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*

Modes de chiffrement

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*
- *La disponibilité?*

Modes de chiffrement

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*
- *La disponibilité?*

Modes de chiffrement

Le mode d'opération définit la façon avec laquelle va-t-on procéder à un chiffrement/déchiffrement. On en cite:

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*
- *La disponibilité?*

Modes de chiffrement

Le mode d'opération définit la façon avec laquelle va-t-on procéder à un chiffrement/déchiffrement. On en cite:

- Algorithmes de chiffrement par block

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*
- *La disponibilité?*

Modes de chiffrement

Le mode d'opération définit la façon avec laquelle va-t-on procéder à un chiffrement/déchiffrement. On en cite:

- Algorithmes de chiffrement par block
- Algorithmes de chiffrement en continu

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*
- *La disponibilité?*

Modes de chiffrement

Le mode d'opération définit la façon avec laquelle va-t-on procéder à un chiffrement/déchiffrement. On en cite:

- Algorithmes de chiffrement par block
  - ECB *Electronic Code Book*
- Algorithmes de chiffrement en continu

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*
- *La disponibilité?*

Modes de chiffrement

Le mode d'opération définit la façon avec laquelle va-t-on procéder à un chiffrement/déchiffrement. On en cite:

- Algorithmes de chiffrement par block
  - ECB *Electronic Code Book*
  - CBC *Cipher Block Chaining*
- Algorithmes de chiffrement en continu

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*
- *La disponibilité?*

Modes de chiffrement

Le mode d'opération définit la façon avec laquelle va-t-on procéder à un chiffrement/déchiffrement. On en cite:

- Algorithmes de chiffrement par block
  - ECB *Electronic Code Book*
  - CBC *Cipher Block Chaining*
- Algorithmes de chiffrement en continu
  - CFB *Cipher Feed Back*

Objectifs de la cryptographie

Principes de la sécurité

- *La confidentialité*
- *L'intégrité*
- *L'authentification*
- *La non-répudiation*
- *La disponibilité?*

Modes de chiffrement

Le mode d'opération définit la façon avec laquelle va-t-on procéder à un chiffrement/déchiffrement. On en cite:

- Algorithmes de chiffrement par block
  - ECB *Electronic Code Book*
  - CBC *Cipher Block Chaining*
- Algorithmes de chiffrement en continu
  - CFB *Cipher Feed Back*
  - OFB *Output Feed Back*

Le mode ECB - Electronic Code Book

Carnet de codage électronique

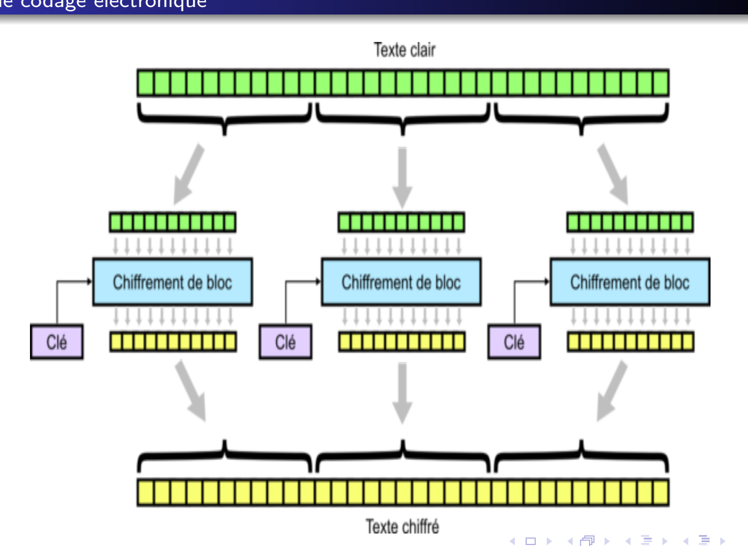


Figure: Mode ECB (wikipédia)

Le mode ECB - Electronic Code Book

Avantages

Désavantage

Le mode ECB - Electronic Code Book

Avantages

- Le traitement (chiffrement ou déchiffrement) de chaque bloc est indépendant des autres blocs

Désavantage

Le mode ECB - Electronic Code Book

Avantages

- Le traitement (chiffrement ou déchiffrement) de chaque bloc est indépendant des autres blocs
- S'il y a une erreur, on demande la retransmission du bloc concerné seulement

Désavantage

Le mode ECB - Electronic Code Book

Avantages

- Le traitement (chiffrement ou déchiffrement) de chaque bloc est indépendant des autres blocs
- S'il y a une erreur, on demande la retransmission du bloc concerné seulement

Désavantage

- S'il y a une répétition dans le texte en clair, elle sera visible sur le texte chiffré

Le mode CBC - Cipher Block Chaining

Chaînage de blocs

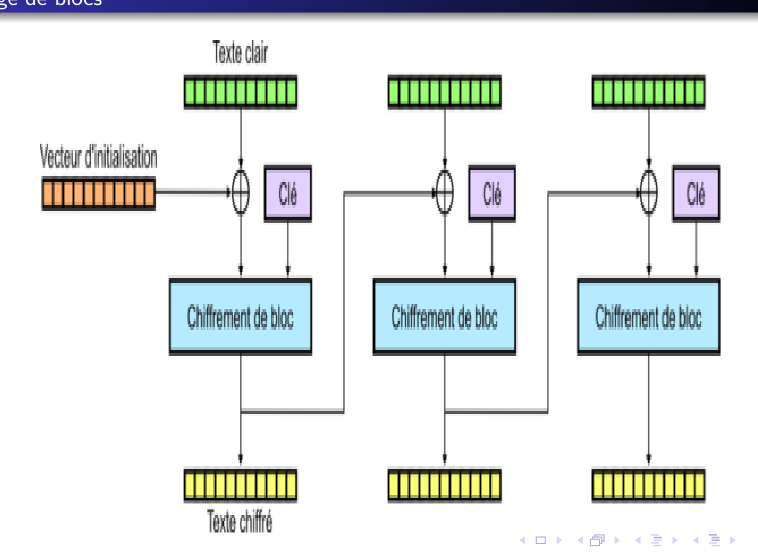


Figure: Mode CBC (wikipédia)

Le mode CBC - Cipher Block Chaining

Avantages

Désavantage

Le mode CBC - Cipher Block Chaining

Avantages

- Les répétitions dans le texte en clair seront masquées

Désavantage

Le mode CBC - Cipher Block Chaining

Avantages

- Les répétitions dans le texte en clair seront masquées

Désavantage

- Une erreur de transmission d'un bit affectera aussi le bit avec lequel il a eu le ou exclusif

Le mode CBC - Cipher Block Chaining

Avantages

- Les répétitions dans le texte en clair seront masquées

Désavantage

- Une erreur de transmission d'un bit affectera aussi le bit avec lequel il a eu le ou exclusif
- Deux premiers blocs pareils de deux textes en clair différents produiront deux premiers blocs pareils dans le texte chiffré

Le mode CFB - Cipher Feed Back

Chiffrement à rétroaction

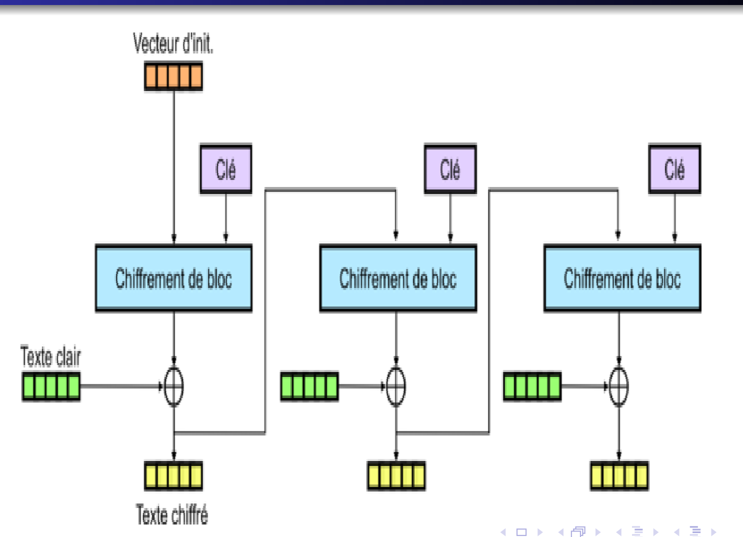
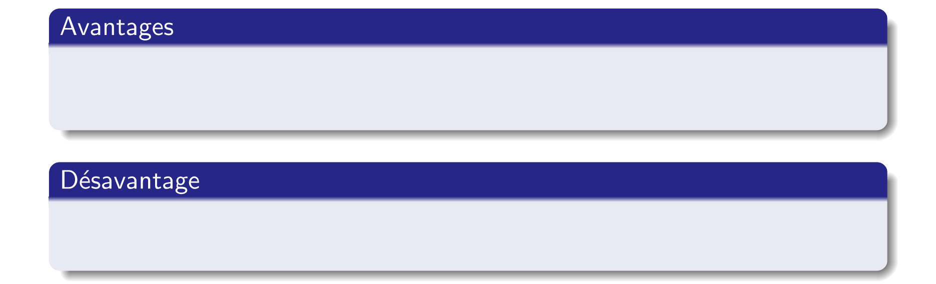


Figure: Mode CFB (wikipédia)

Le mode CFB - Cipher Feed Back



Le mode CFB - Cipher Feed Back

Avantages

- Chiffrement par flot de donnée

Désavantage

Le mode CFB - Cipher Feed Back

Avantages

- Chiffrement par flot de donnée
- Masquage des répétitions du texte en clair

Désavantage

Le mode CFB - Cipher Feed Back

Avantages

- Chiffrement par flot de donnée
- Masquage des répétitions du texte en clair

Désavantage

- Une erreur de transmission d'un bit affectera aussi le bit avec lequel il a eu le ou exclusif

Le mode OFB - Output Feed Back

Rétroaction de sortie

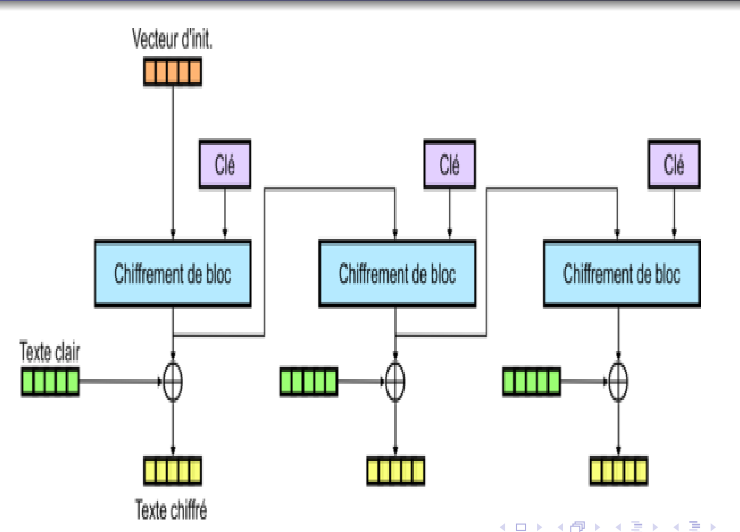


Figure: Mode OFB (wikipédia)

Le mode OFB - Output Feed Back

Avantages

Le mode OFB - Output Feed Back

Avantages

- Les répétitions dans le texte en clair seront masquées

Le mode OFB - Output Feed Back

Avantages

- Les répétitions dans le texte en clair seront masquées
- Une erreur de transmission n'affecte que le bloc concerné

Plan

La cryptographie symétrique

Scénario

La cryptographie symétrique

Autrement appelé: Cryptographie à clé privé

Scénario

La cryptographie symétrique

Autrement appelé: Cryptographie à clé privé

Même clé utilisée pour le chiffrement et le déchiffrement

Scénario

La cryptographie symétrique

Autrement appelé: Cryptographie à clé privé

Même clé utilisée pour le chiffrement et le déchiffrement

Scénario

- L'émetteur et le récepteur partage une clé privé depuis un canal sûr

La cryptographie symétrique

Autrement appelé: Cryptographie à clé privé

Même clé utilisée pour le chiffrement et le déchiffrement

Scénario

- L'émetteur et le récepteur partage une clé privé depuis un canal sûr
- L'émetteur chiffre le message avec la clé et envoie le résultat

La cryptographie symétrique

Autrement appelé: Cryptographie à clé privé

Même clé utilisée pour le chiffrement et le déchiffrement

Scénario

- L'émetteur et le récepteur partage une clé privé depuis un canal sûr
- L'émetteur chiffre le message avec la clé et envoie le résultat
- Le récepteur déchiffre ce qu'il a reçu avec la clé déjà partagée

La cryptographie symétrique

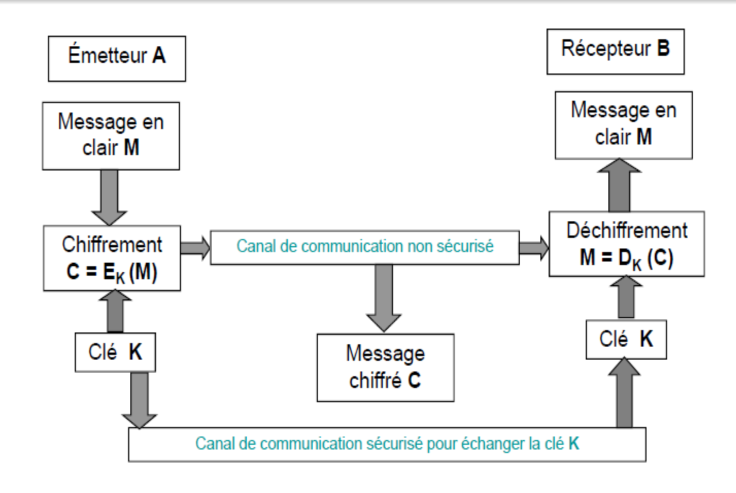


Figure: Cryptographie symétrique

La cryptographie symétrique

Avantages

Désavantages

Exemples

La cryptographie symétrique

Avantages

- Rapidité de chiffrement et de déchiffrement

Désavantages

Exemples

La cryptographie symétrique

Avantages

- Rapidité de chiffrement et de déchiffrement
- Confidentialité des l'information (local ou en transit)

Désavantages

Exemples

La cryptographie symétrique

Avantages

- Rapidité de chiffrement et de déchiffrement
- Confidentialité des l'information (local ou en transit)

Désavantages

- Difficulté de partage de la clé

Exemples

La cryptographie symétrique

Avantages

- Rapidité de chiffrement et de déchiffrement
- Confidentialité des l'information (local ou en transit)

Désavantages

- Difficulté de partage de la clé
- Si vous êtes dans un réseau de N personnes, il vous faut N-1 clés

Exemples

La cryptographie symétrique

Avantages

- Rapidité de chiffrement et de déchiffrement
- Confidentialité des l'information (local ou en transit)

Désavantages

- Difficulté de partage de la clé
- Si vous êtes dans un réseau de N personnes, il vous faut N-1 clés

Exemples

DES, 3DES, IDEA, AES

La cryptographie asymétrique

Scénario

La cryptographie asymétrique

Autrement appelé: Cryptographie à clé publique

Scénario

La cryptographie asymétrique

Autrement appelé: Cryptographie à clé publique

Elle met en jeux une paire de clés pour chaque utilisateur (K,K')

Scénario

La cryptographie asymétrique

Autrement appelé: Cryptographie à clé publique

Elle met en jeux une paire de clés pour chaque utilisateur (K,K')

- L'une pour le chiffrement **K** (clé publique)

Scénario

La cryptographie asymétrique

Autrement appelé: Cryptographie à clé publique

Elle met en jeux une paire de clés pour chaque utilisateur (K,K')

- L'une pour le chiffrement **K** (clé publique)
- L'autre pour le déchiffrement **K'** (clé privée)

Scénario

La cryptographie asymétrique

Autrement appelé: Cryptographie à clé publique

Elle met en jeux une paire de clés pour chaque utilisateur (K,K')

L'une pour le chiffrement **K** (clé publique)
L'autre pour le déchiffrement **K'** (clé privée)

Scénario

- L'émetteur et le récepteur génèrent chacun une paire de clés

La cryptographie asymétrique

Autrement appelé: Cryptographie à clé publique

Elle met en jeux une paire de clés pour chaque utilisateur (K,K')

L'une pour le chiffrement **K** (clé publique)
L'autre pour le déchiffrement **K'** (clé privée)

Scénario

- L'émetteur et le récepteur génèrent chacun une paire de clés
- L'émetteur chiffre le message avec la clé publique du récepteur et envoie le résultat

La cryptographie asymétrique

Autrement appelé: Cryptographie à clé publique

Elle met en jeux une paire de clés pour chaque utilisateur (K,K')

L'une pour le chiffrement **K** (clé publique)
L'autre pour le déchiffrement **K'** (clé privée)

Scénario

- L'émetteur et le récepteur génèrent chacun une paire de clés
- L'émetteur chiffre le message avec la clé publique du récepteur et envoie le résultat
- Le récepteur déchiffre ce qu'il a reçu avec sa clé privé

La cryptographie asymétrique

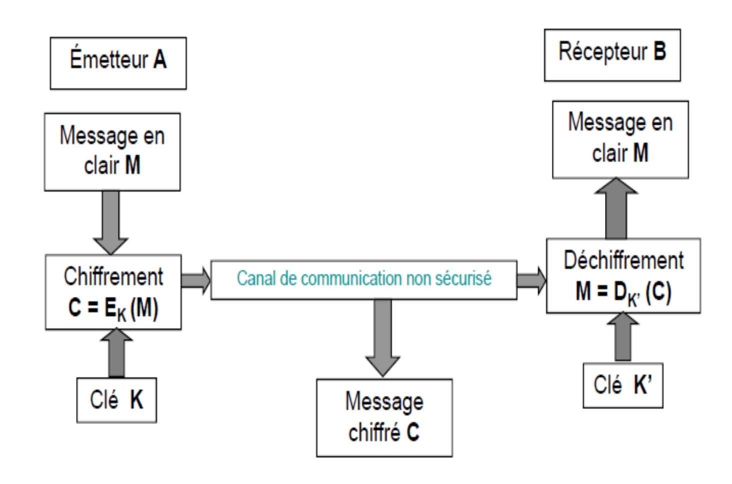


Figure: Cryptographie asymétrique

La cryptographie asymétrique

Avantages

Désavantages

Exemples

La cryptographie asymétrique

Avantages

- Les clés publiques peuvent être échangées dans un canal non sûr (voire publiées)

Désavantages

Exemples

La cryptographie asymétrique

Avantages

- Les clés publiques peuvent être échangées dans un canal non sûr (voire publiées)
- Le nombre de clés croît linéairement

Désavantages

Exemples

La cryptographie asymétrique

Avantages

- Les clés publiques peuvent être échangées dans un canal non sûr (voire publiées)
- Le nombre de clés croît linéairement
- Confidentialité, intégrité, ...

Désavantages

Exemples

La cryptographie asymétrique

Avantages

- Les clés publiques peuvent être échangées dans un canal non sûr (voire publiées)
- Le nombre de clés croît linéairement
- Confidentialité, intégrité, ...

Désavantages

- Temps de calcul

Exemples

La cryptographie asymétrique

Avantages

- Les clés publiques peuvent être échangées dans un canal non sûr (voire publiées)
- Le nombre de clés croît linéairement
- Confidentialité, intégrité, ...

Désavantages

- Temps de calcul
- Validité des clés publiques

Exemples

La cryptographie asymétrique

Avantages

- Les clés publiques peuvent être échangées dans un canal non sûr (voire publiées)
- Le nombre de clés croît linéairement
- Confidentialité, intégrité, ...

Désavantages

- Temps de calcul
- Validité des clés publiques

Exemples

- RSA, Diffie-hellman, Elgamal

La cryptographie hybride

Hybride?

Scénario

La cryptographie hybride

Hybride?

Combinaison des deux méthodes (symétrique et asymétrique)

Scénario

La cryptographie hybride

Hybride?

Combinaison des deux méthodes (symétrique et asymétrique)

Scénario

- L'émetteur et le récepteur utilisent l'aspect symétrique pour envoyer une clé privé (clé de session)

La cryptographie hybride

Hybride?

Combinaison des deux méthodes (symétrique et asymétrique)

Scénario

- L'émetteur et le récepteur utilisent l'aspect symétrique pour envoyer une clé privé (clé de session)
- L'émetteur chiffre la clé de session avec la clé publique du récepteur et lui envoie le résultat

La cryptographie hybride

Hybride?

Combinaison des deux méthodes (symétrique et asymétrique)

Scénario

- L'émetteur et le récepteur utilisent l'aspect symétrique pour envoyer une clé privé (clé de session)
- L'émetteur chiffre la clé de session avec la clé publique du récepteur et lui envoie le résultat
- Le récepteur déchiffre ce qu'il a reçu avec sa clé privé pour trouver la clé de session

La cryptographie hybride

Hybride?

Combinaison des deux méthodes (symétrique et asymétrique)

Scénario

- L'émetteur et le récepteur utilisent l'aspect symétrique pour envoyer une clé privé (clé de session)
- L'émetteur chiffre la clé de session avec la clé publique du récepteur et lui envoie le résultat
- Le récepteur déchiffre ce qu'il a reçu avec sa clé privé pour trouver la clé de session
- L'émetteur et le récepteur passent à une méthode de cryptographie symétrique pour la suite de la communication

Plan

Définition



Définition

Définition

Une fonction de hachage (ou une fonction de condensation) est *une fonction à sens unique sans collision* qui sert à convertir une chaîne binaire de longueur quelconque en une autre de taille considérablement inférieure.

Caractéristiques

Exemples

Définition

Définition

Une fonction de hachage (ou une fonction de condensation) est *une fonction à sens unique sans collision* qui sert à convertir une chaîne binaire de longueur quelconque en une autre de taille considérablement inférieure.

Caractéristiques

- La chaîne résultante est appelée *une empreinte* (condensé, haché, digest)

Exemples

Définition

Définition

Une fonction de hachage (ou une fonction de condensation) est *une fonction à sens unique sans collision* qui sert à convertir une chaîne binaire de longueur quelconque en une autre de taille considérablement inférieure.

Caractéristiques

- La chaîne résultante est appelée *une empreinte* (condensé, haché, digest)
- Une fonction à sens unique est une fonction difficile à inverser

Exemples

Définition

Définition

Une fonction de hachage (ou une fonction de condensation) est *une fonction à sens unique sans collision* qui sert à convertir une chaîne binaire de longueur quelconque en une autre de taille considérablement inférieure.

Caractéristiques

- La chaîne résultante est appelée *une empreinte* (condensé, haché, digest)
- Une fonction à sens unique est une fonction difficile à inverser
- Une fonction sans collision pour dire que pour n'importe quelle pair de chaînes, il est impossible de trouver la même empreinte

Exemples

Définition

Définition

Une fonction de hachage (ou une fonction de condensation) est *une fonction à sens unique sans collision* qui sert à convertir une chaîne binaire de longueur quelconque en une autre de taille considérablement inférieure.

Caractéristiques

- La chaîne résultante est appelée *une empreinte* (condensé, haché, digest)
- Une fonction à sens unique est une fonction difficile à inverser
- Une fonction sans collision pour dire que pour n'importe quelle pair de chaînes, il est impossible de trouver la même empreinte

Exemples

MD5, SHA, Whirlpool

Application des fonctions de hachage

- L'intégrité
- L'authentification

Application des fonctions de hachage

Contrôle d'intégrité

Scénario

Application des fonctions de hachage

Contrôle d'intégrité

Scénario

- L'expéditeur envoie le message accompagné de son haché

Application des fonctions de hachage

Contrôle d'intégrité

Scénario

- L'expéditeur envoie le message accompagné de son haché
- Le récepteur hache le message reçu et compare le haché obtenu avec le haché reçu

Application des fonctions de hachage

Contrôle d'intégrité

Scénario

- L'expéditeur envoie le message accompagné de son haché
- Le récepteur hache le message reçu et compare le haché obtenu avec le haché reçu
- Mais comment être certain de la provenance du haché?

Application des fonctions de hachage

Signature numérique

Définition

[a] Elle dépend du message

Scénario

Application des fonctions de hachage
Signature numérique

Définition

Une signature (non réutilisable[a]) numérique est un haché chiffré par une clé privé dans le but d'assurer l'authenticité de la provenance du message.

[a] Elle dépend du message

Scénario

Application des fonctions de hachage

Signature numérique

Définition

Une signature (non réutilisable[a]) numérique est un haché chiffré par une clé privé dans le but d'assurer l'authenticité de la provenance du message.

[a] Elle dépend du message

Scénario

- L'expéditeur chiffre à l'aide de sa clé privé le haché du message qu'il veut envoyer

Application des fonctions de hachage

Signature numérique

Définition

Une signature (non réutilisable[a]) numérique est un haché chiffré par une clé privé dans le but d'assurer l'authenticité de la provenance du message.

[a] Elle dépend du message

Scénario

- L'expéditeur chiffre à l'aide de sa clé privé le haché du message qu'il veut envoyer
- Le haché ainsi signé accompagne le message dans la transmission

Application des fonctions de hachage
Signature numérique

Définition

Une signature (non réutilisable[a]) numérique est un haché chiffré par une clé privé dans le but d'assurer l'authenticité de la provenance du message.

[a]Elle dépend du message

Scénario

- L'expéditeur chiffre à l'aide de sa clé privé le haché du message qu'il veut envoyer
- Le haché ainsi signé accompagne le message dans la transmission
- Le récepteur commence par déchiffré le haché avant de le comparer avec le hache du message reçu

Plan

Motivations



Motivations

- Protéger les clés publiques contre les falsifications

Motivations

- Protéger les clés publiques contre les falsifications
- Affirmer l'appartenance d'une clé publique à un détenteur

Motivations

- Protéger les clés publiques contre les falsifications
- Affirmer l'appartenance d'une clé publique à un détenteur

- Alors, comment gérer les certificats dans un environnement distribué?

Motivations

- Protéger les clés publiques contre les falsifications
- Affirmer l'appartenance d'une clé publique à un détenteur

- Alors, comment gérer les certificats dans un environnement distribué?
- Deux méthodes:

Motivations

- Protéger les clés publiques contre les falsifications
- Affirmer l'appartenance d'une clé publique à un détenteur

- Alors, comment gérer les certificats dans un environnement distribué?
- Deux méthodes:
    - PKI (*Public Key Infrastructure*)

Motivations

- Protéger les clés publiques contre les falsifications
- Affirmer l'appartenance d'une clé publique à un détenteur

- Alors, comment gérer les certificats dans un environnement distribué?
- Deux méthodes:
  - PKI (*Public Key Infrastructure*)
  - OpenPGP (*Pretty Good Privacy*)

Public Key Infrastructure

Définition

Définition

La gestion des certificats numériques

Public Key Infrastructure

Définition

Définition

Une PKI est un ensemble de mécanismes qui permet de vérifier, valider et gérer les certificats numériques.

La gestion des certificats numériques

Public Key Infrastructure

Définition

Définition

Une PKI est un ensemble de mécanismes qui permet de vérifier, valider et gérer les certificats numériques.

La gestion des certificats numériques

- Fabrication des pairs de clés

Public Key Infrastructure

Définition

Définition

Une PKI est un ensemble de mécanismes qui permet de vérifier, valider et gérer les certificats numériques.

La gestion des certificats numériques

- Fabrication des pairs de clés
- Certification des clés publiques

Public Key Infrastructure

Définition

Définition

Une PKI est un ensemble de mécanismes qui permet de vérifier, valider et gérer les certificats numériques.

La gestion des certificats numériques

- Fabrication des pairs de clés
- Certification des clés publiques
- Publication des certificats

Public Key Infrastructure
Définition

Définition

Une PKI est un ensemble de mécanismes qui permet de vérifier, valider et gérer les certificats numériques.

La gestion des certificats numériques

- Fabrication des pairs de clés
- Certification des clés publiques
- Publication des certificats
- Révocation de certificats

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

[a] CSR - Certificate Signing Request

Public Key Infrastructure
Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
- **Une autorité de certification**
- **Un annuaire**

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
  - Vérifier les demandes d'enregistrement[a] d'un nouvel utilisateur.
- **Une autorité de certification**
- **Un annuaire**

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
  - Vérifier les demandes d'enregistrement[a] d'un nouvel utilisateur.
  - Transférer les demandes éligibles à l'autorité de certification
- **Une autorité de certification**
- **Un annuaire**

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
  - Vérifier les demandes d'enregistrement[a] d'un nouvel utilisateur.
  - Transférer les demandes éligibles à l'autorité de certification
- **Une autorité de certification**
  - Gérer les certificats
- **Un annuaire**

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
  - Vérifier les demandes d'enregistrement[a] d'un nouvel utilisateur.
  - Transférer les demandes éligibles à l'autorité de certification
- **Une autorité de certification**
  - Gérer les certificats
  - Signer les certificats qu'elle délivre
- **Un annuaire**

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
  - Vérifier les demandes d'enregistrement[a] d'un nouvel utilisateur.
  - Transférer les demandes éligibles à l'autorité de certification
- **Une autorité de certification**
  - Gérer les certificats
  - Signer les certificats qu'elle délivre
  - Mettre à jour la liste des certificats qui sont encore valide
- **Un annuaire**

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
  - Vérifier les demandes d'enregistrement[a] d'un nouvel utilisateur.
  - Transférer les demandes éligibles à l'autorité de certification
- **Une autorité de certification**
  - Gérer les certificats
  - Signer les certificats qu'elle délivre
  - Mettre à jour la liste des certificats qui sont encore valide
- **Un annuaire**
  - Il est indépendant de la PKI (compatible avec les protocoles X.509 et LDAP)

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
  - Vérifier les demandes d'enregistrement[a] d'un nouvel utilisateur.
  - Transférer les demandes éligibles à l'autorité de certification
- **Une autorité de certification**
  - Gérer les certificats
  - Signer les certificats qu'elle délivre
  - Mettre à jour la liste des certificats qui sont encore valide
- **Un annuaire**
  - Il est indépendant de la PKI (compatible avec les protocoles X.509 et LDAP)
  - Stocker les certificats (valides et révoqués)

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Composantes d'une PKI

Composantes d'une PKI

Les principales composantes d'une PKI sont:

- **Une autorité d'enregistrement**
  - Vérifier les demandes d'enregistrement[a] d'un nouvel utilisateur.
  - Transférer les demandes éligibles à l'autorité de certification
- **Une autorité de certification**
  - Gérer les certificats
  - Signer les certificats qu'elle délivre
  - Mettre à jour la liste des certificats qui sont encore valide
- **Un annuaire**
  - Il est indépendant de la PKI (compatible avec les protocoles X.509 et LDAP)
  - Stocker les certificats (valides et révoqués)
  - Stocker les clés privés (dans le cadre de recouvrement de clé)

[a] CSR - Certificate Signing Request

Public Key Infrastructure

Architecture PKI

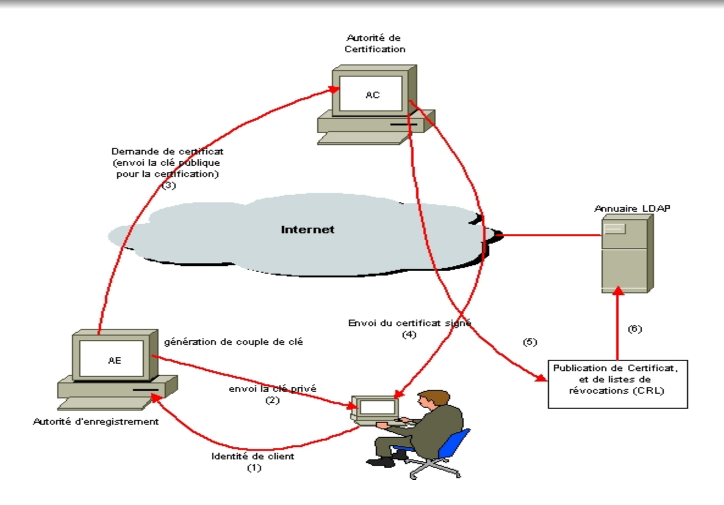


Figure: Architecture PKI

Public Key Infrastructure

Les certificats

Définition

Exemple (X.509)

Public Key Infrastructure
Les certificats

Définition

Un certificat numérique identifie un utilisateur. Il contient:

Exemple (X.509)

Public Key Infrastructure

Les certificats

Définition

Un certificat numérique identifie un utilisateur. Il contient:

- Des informations personnelles

Exemple (X.509)

Public Key Infrastructure

Les certificats

Définition

Un certificat numérique identifie un utilisateur. Il contient:

- Des informations personnelles
- La clés publique

Exemple (X.509)

Public Key Infrastructure

Les certificats

Définition

Un certificat numérique identifie un utilisateur. Il contient:

- Des informations personnelles
- La clés publique
- La signature numérique de l'autorité de certification qui l'a émise

Exemple (X.509)

Public Key Infrastructure

Les certificats

Définition

Un certificat numérique identifie un utilisateur. Il contient:

- Des informations personnelles
- La clés publique
- La signature numérique de l'autorité de certification qui l'a émise
- Sa date de validité

Exemple (X.509)

Public Key Infrastructure

Les certificats

Définition

Un certificat numérique identifie un utilisateur. Il contient:

- Des informations personnelles
- La clés publique
- La signature numérique de l'autorité de certification qui l'a émise
- Sa date de validité

Exemple (X.509)

- Allez aux préférences du navigateur web *firefox* par exemple

Public Key Infrastructure
Les certificats

Définition

Un certificat numérique identifie un utilisateur. Il contient:

- Des informations personnelles
- La clés publique
- La signature numérique de l'autorité de certification qui l'a émise
- Sa date de validité

Exemple (X.509)

- Allez aux préférences du navigateur web *firefox* par exemple
- L'onglet *Avancé*

Public Key Infrastructure

Les certificats

Définition

Un certificat numérique identifie un utilisateur. Il contient:

- Des informations personnelles
- La clés publique
- La signature numérique de l'autorité de certification qui l'a émise
- Sa date de validité

Exemple (X.509)

- Allez aux préférences du navigateur web *firefox* par exemple
- L'onglet *Avancé*
- Afficher les certificats